التعاكس التربيعي
Quadratic Reciprocity

ما نريده هنا هو أن نحدد بالضبط ، لعدد معطى a ، أي الأعداد الأولية p يكون لها a راسب تربيعي. في الفصل السابق أوجدنا حل هذه المسألة عندما $a=-1$, $a=2$. وجدنا في كلتا الحالتين أنه بإمكاننا تحديد أي قيمة لـ a تجعله راسباً تربيعيًّا قياس p ، وذلك من خلال النظر إلى p قياس m لقيمة صغرى للعدد m ، وبشكل محدد عندما $m=4$ أو $m=8$.

نريد الآن معالجة السؤال بالنسبة إلى رمز لجندر $\left(\dfrac{a}{p}\right)$ لقيم أخرى لـ a .

على سبيل المثال ، افرض أننا نريد حساب $\left(\dfrac{70}{p}\right)$. نستطيع استخدام قوانين ضرب الراسب التربيعي (فصل 23) لحساب :

$$\begin{aligned}\left(\frac{70}{p}\right)&=\left(\frac{2\cdot5\cdot7}{p}\right)\\&=\left(\frac{2}{p}\right)\left(\frac{3}{p}\right)\left(\frac{7}{p}\right)\end{aligned}$$

نحن نعرف كيف نجد $\left(\frac{2}{p}\right)$ ؛ لذلك سوف نهتم بإيجاد $\left(\frac{5}{p}\right)$, $\left(\frac{7}{p}\right)$.

بشكل عام، إذا أردنا حساب $\left(\frac{a}{p}\right)$ لأي عدد a ، فيمكننا أن نبدأ بتحليل a إلى حاصل ضرب عوامله الأولية،

$$a = q_1 q_2 \ldots q_r$$

(لا يوجد مشكلة إذا كان بعض قيم q_i نفسها). عندئذ فإن قوانين ضرب الراسب التربيعي تعطي:

$$\left(\frac{a}{p}\right) = \left(\frac{q_1}{p}\right)\left(\frac{q_2}{p}\right)\ldots\left(\frac{q_r}{p}\right)$$

إن المغزى من هذه القصة هو: إذا كنا نعرف كيف نحسب $\left(\frac{a}{p}\right)$ للأعداد الأولية q ، فإننا نعرف كيف نحسب $\left(\frac{a}{p}\right)$ لأي a [1]. بما أننا لم نعمل شيئاً حتى الآن يخبرنا أي شيء عن $\left(\frac{q}{p}\right)$ (q له قيمة ثابتة و p له قيم متغيرة)، فإن الوقت قد حان لجمع بعض البيانات واستخدامها لعمل بعض التخمينات. الجدول التالي يعطي قيمة رمز لجندر $\left(\frac{q}{p}\right)$ لجميع الأعداد الأولية $p\ ,\ q \le 37$.

---

(١) إن الأعداد الأولية تشكل لبنات البناء الأساسية لنظرية الأعداد، وعليه إذا كان باستطاعتك حل مسألة من الأعداد الأولية، فإنك غالباً ما تستطيع حلها لكل الأعداد.

q/p	3	5	7	11	13	17	19	23	29	31	37
3		−1	1	−1	1	−1	1	−1	−1	1	1
5	−1		−1	1	−1	−1	1	−1	1	1	−1
7	−1	−1		1	−1	−1	−1	1	1	−1	1
11	1	1	−1		−1	−1	−1	1	−1	1	1
13	1	−1	−1	−1		1	−1	1	1	−1	−1
17	−1	−1	−1	−1	1		1	−1	−1	−1	−1
19	−1	1	1	1	−1	1		1	−1	−1	−1
23	1	−1	−1	−1	1	−1	−1		1	1	−1
29	−1	1	1	−1	1	−1	−1	1		−1	−1
31	−1	1	1	−1	−1	−1	1	−1	−1		−1
37	1	−1	1	1	−1	−1	−1	−1	−1	−1	

قيمة رمز لجندر $\left(\dfrac{q}{p}\right)$

قبل أن نسترسل في القراءة، يجب عليك أخذ بعض الوقت لدراسة هذا الجدول ومحاولة إيجاد بعض الأنماط. لا تقلق إذا لم تكتشف الجواب مباشرة، إن أهم نمط مختبئ

في هذا الجدول هو نمط دقيق إلى حد ما. ولكنك ستجد أن جهدك المبذول لاكتشاف هذا النمط لوحدك يستحق منك هذا العناء؛ لأنك عندها ستكون قد شاركت لجندر وجاوس لذة هذا الاكتشاف.

الآن بعد أن وضعت صيغة لتخمينك، سوف نقوم معاً بفحص الجدول. سنقوم بمقارنة الصفوف بالأعمدة أو بمقارنة المدخلات عند عمل انعكاس حول قطر الجدول. فعلى سبيل المثال، الصف $p=5$:

q	3	5	7	11	13	17	19	23	29	31	37
$(q/5)$	-1		-1	1	-1	-1	1	-1	1	1	-1

نفس الشيء مع العمود $q=5$

p	3	5	7	11	13	17	19	23	29	31	37
$(5/p)$	-1		-1	1	-1	-1	1	-1	1	1	-1

من هذا الجدول نتوقع أن:

$$\left(\frac{5}{p}\right)=\left(\frac{p}{5}\right)$$

لكل الأعداد الأولية p . هل ترى كم من المفيد أن نحصل على قانون مثل هذا؟ نحن نبحث عن طريقة لحساب رمز لجندر $\left(\frac{5}{p}\right)$ ، إنها مسألة صعبة ، لكن من السهل حساب رمز لجندر $\left(\frac{p}{5}\right)$ ؛ لأنه يعتمد فقط على p قياس 5. بكلمات أخرى ، نحن نعلم أن :

$$\left(\frac{p}{5}\right)=\begin{cases}1\ , & \text{if} \quad p\equiv 1 \ \ or \ \ 4 \pmod 5 \\ \\ -1\ , & \text{if} \quad p\equiv 2 \ \ or \ \ 3 \pmod 5\end{cases}$$

لذلك إذا كان تخميننا $\left(\frac{p}{5}\right)=\left(\frac{5}{p}\right)$ صحيح ، فإننا نعلم ، على سبيل المثال ، أن 5 راسب غير تربيعي قياس 3593 ؛ لأن :

$$\left(\frac{5}{3593}\right)=\left(\frac{3593}{5}\right)=\left(\frac{3}{5}\right)=-1$$

نفس الشيء :

$$\left(\frac{5}{3889}\right)=\left(\frac{3889}{5}\right)=\left(\frac{4}{5}\right)=1 ،$$

إذاً 5 يجب أن تكون راسباً تربيعيًّا قياس 3889 ، وبكل تأكيد نجد أن : $5\equiv 2901^2 \pmod{3889}$.

بتشجيع من هذا النجاح ، فإننا قد نتوقع أن :

$$\left(\frac{q}{p}\right)=\left(\frac{p}{q}\right)$$

لكل الأعداد الأولية p , q . لسوء الحظ ، فإن هذا غير صحيح حتى بالنسبة للصف الأول والعمود الأول من هذا الجدول. مثلاً :

$$\left(\frac{7}{3}\right)=1 \quad , \quad \left(\frac{3}{7}\right)=-1$$

لذلك أحياناً يكون $\left(\frac{q}{p}\right)$ مساوياً $\left(\frac{p}{q}\right)$ ، وأحياناً يساوي $-\left(\frac{p}{q}\right)$.

الجدول التالي سيساعدنا على إيجاد قانون يوضح متى يكونان نفس الشيء ومتى يكونان متعاكسان في الإشارة.

q/p	3	5	7	11	13	17	19	23	29	31	37
3		~	★	★	~	~	★	★	~	★	~
5	~		~	~	~	~	~	~	~	~	~
7	★	~		★	~	~	★	★	~	★	~
11	★	~	★		~	~	★	★	~	★	~
13	~	~	~	~		~	~	~	~	~	~
17	~ ★	~	~ ★	~ ★	~		~	~ ★	~	~ ★	~
19	★	~	★	★	~	~	★		~	★	~
23	~	~	~	~	~	~	~	~		~	~
29	★	~	★	★	~	~	★	★	~		~
31	~	~	~	~	~	~	~	~	~	~	

جدول وضع فيه ~ عندما $\left(\frac{p}{q}\right)=\left(\frac{q}{p}\right)$ **و ★ عندما** $\left(\frac{p}{q}\right)=-\left(\frac{q}{p}\right)$

بالنظر لهذا الجدول، نستطيع اختيار الأعداد الأولية التي صفوفها وأعمدتها تحوي بالكامل الرمز ~ وهي:

$$p = 5,13,17,29,37$$

الأعداد الأولية التي صفوفها وأعمدتها ليست بالضبط نفسها (بمعنى، الصفوف والأعمدة تحوي ★) هي:

$$p = 3,7,11,19,23,31$$

من خبرتنا السابقة، لا يوجد غموض في هذه القوائم، فالأولى تضم الأعداد الأولية التي تطابق 1 قياس 4، والأخيرة تضم الأعداد الأولية التي تطابق 3 قياس 4.

وعليه؛ فإن تخميننا الأول قد يكون أنه إذا كان $p \equiv 1 \pmod 4$ أو إذا كان $q \equiv 1 \pmod 4$ فإن الصفوف والأعمدة تكون نفسها. ويمكننا كتابة ذلك بإستخدام رمز لجندر.

تخمين

إذا كان $p \equiv 1 \pmod 4$ *أو* $q \equiv 1 \pmod 4$ *فإن* $\left(\dfrac{p}{q}\right) = \left(\dfrac{q}{p}\right)$.

ماذا يحدث لو أن كل من p , q يطابق 3 قياس 4؟ بالنظر إلى الجدول، نجد أن $\left(\dfrac{q}{p}\right)$, $\left(\dfrac{p}{q}\right)$ متعاكسان دائماً. إن هذا يقودنا لعمل التخمين الإضافي التالي:

تخمين

إذا كان $p \equiv 3(\bmod 4)$ *و* $q \equiv 3(\bmod 4)$ *؛ فإن* $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$.

هاتان العلاقتان التخمينيتان تشكلان جوهر قانون التعاكس التربيعي.

نظرية (١, ٢٥) (قانون التعاكس التربيعي)

ليكن p , q *عددين أوليين فرديين مختلفين*

$$\left(\frac{-1}{p}\right) = \begin{cases} 1\ , & \text{if} \quad p \equiv 1(\bmod 4) \\ -1\ , & \text{if} \quad p \equiv 3(\bmod 4) \end{cases}$$

$$\left(\frac{2}{p}\right) = \begin{cases} 1\ , & \text{if} \quad p \equiv 1 \text{ or } 7(\bmod 8) \\ -1\ , & \text{if} \quad p \equiv 3 \text{ or } 5(\bmod 8) \end{cases}$$

$$\left(\frac{q}{p}\right) = \begin{cases} \left(\frac{q}{p}\right), & \text{if} \quad q \equiv 1(\bmod 4) \text{ or } p \equiv 1(\bmod 4) \\ -\left(\frac{p}{q}\right), & \text{if} \quad q \equiv 1(\bmod 4) \text{ and } p \equiv 3(\bmod 4) \end{cases}$$

سنكون قانعين بالحصول على برهان قانون التعاكس التربيعي للمقدارين $\left(\frac{-1}{p}\right)$, $\left(\frac{2}{p}\right)$ ولن نعطي البرهان العام للمقدار $\left(\frac{p}{q}\right)$. إن هناك الكثير من البراهين على قانون التعاكس التربيعي ، أحدها يشبه كثيراً برهاننا للمقدار $\left(\frac{2}{p}\right)$ في

الفصل السابق[١] . إن أويلر Euler و لاجرانج Lagrange كانا أول من صاغ قانون التعاكس التربيعي ، ولكنه بقي لجاوس ليعطي عليه أول برهان في بحثه الشهير "التقارير الحسابية" في 1801. لقد اكتشف جاوس القانون بنفسه عندما كان عمره 19 سنة ، وفي خلال حياته أوجد له سبعة براهين مختلفة ! وفي وقت لاحق قام الرياضيون في القرن التاسع عشر بصياغة برهان قانوني التعاكس التكعيبي والرباعي "Cubic and Quartic Reciproeity Laws" ، وهذان القانونان كانا جزءاً من "نظرية حقل الفئة" التي طُوِرت على يد "ديفيد هيلبرت" David Hilbert ، "إيميل ارتن" Emil Artin وآخرين من عام 1890 وحتى 1930. لقد قام عدد من الرياضيين في ستينات وسبعينات القرن العشرين بصياغة سلسلة من التخمينات ساهمت إلى حد كبير بتعميم ''نظرية حقل الفئة'' وأصبحت تعرف في يومنا هذا "برنامج لانجلاند" Langlands Program . إن النظرية الأساسية التي برهنت على يد "أندرو ويلز" Andrew Wiles في عام 1995 هي جزء صغير من "برنامج لانجلاند" ، كونها كافية لحل "نظرية فيرما الأخيرة".

إن قانون التعاكس التربيعي ليس عبارة نظرية جميلة ودقيقة فقط ، بل هو أيضاً أداة تطبيقية لتحديد فيما إذا كان العدد راسباً تربيعيًّا أم لا. وبشكل أساسي ، يجعلنا نقلب رمز لجندر $\left(\dfrac{q}{p}\right)$ ونستبدله بالمقدار $\pm\left(\dfrac{p}{q}\right)$. وبعد ذلك يمكننا اختزال p قياس q ونعيد نفس الإجراء. وهذا يقود إلى رموز لجندر بمدخلات أصغر وأصغر ، لنصل في النهاية إلى رموز لجندر يمكننا حسابها. هنا مثال تفصيلي مع التوضيح لكل خطوة.

---

(١) يمكنك إيجاد هذا البرهان في الفصل الثالث من كتاب ''دافينيورت'' Davenport المدهش بعنوان ''حسابات عليا'' جامعة كامبريدج ، 1952 ، الصفحة 7 سنة 1999.

"كارل فردريك جاوس" Karl Friedrich Gauss (1855 – 1777)

كارل فردريك جاوس هو أحد أعظم الرياضيين على مر العصور، ويمكن القول إنه أفضل من بحث في نظرية الأعداد. عندما كان طفلاً ، كان معجزة رياضية. أعماله وإنجازاته أثارت إعجاب عائلته وأصدقائه، وأساتذته، ومواهبه الرياضية نمت مع نموه.

أكثر أعماله المؤثرة في نظرية الأعداد نشر سنة 1801 تحت عنوان ''التقارير الحسابية''. فقد احتوى من بين ما احتوى على نظرية التعاكس التربيعي وعلى تمثيل الأعداد بالشكل الثنائي.

كثير من الموضوعات التي احتوتها تقارير جاوس كانت سابقة لعصرها، وهذا العمل بحد ذاته زود الباحثين في الجانب النظري في نظرية الأعداد بأساليب اتبعوها فيما بعد خلال ذلك القرن التاسع عشر والنصف الأول من القرن العشرين. وبالإضافة إلى عمله في نظرية الأعداد، فقد قام جاوس بعمل إسهامات أساسية في كثير من فروع الرياضيات، منها الهندسة والمعادلات التفاضلية. أيضاً قام جاوس بعمل كثير من الاكتشافات في الفيزياء والفلك، من ضمنها طريقة لحساب الأفلاك، والذي استخدمه لحساب موقع الكوكب المكتشف حديثاً "سيرس" Ceres وذلك في عام 1801. لقد قام بنشر أبحاث عديدة في مجالات مختلفة، مثل علم البلوريات، البصريات، وفيزياء الموائع، واخترع مع "ويليام وبر" Wilhelm Weber عام 1833 التلغراف الكهرومغناطيسي. لقد نشر جاوس 155 عنوان خلال حياته، لكن حياته العملية كانت استثنائية، حيث إن مجموعة أعماله ظهرت في الفترة ما بين 1863 و 1933 .

$$\left(\frac{14}{137}\right)=\left(\frac{2}{137}\right)\left(\frac{7}{137}\right)$$ قانون ضرب الراسب

$$=\left(\frac{7}{137}\right)$$ من قانون التعاكس التربيعي $1=\left(\frac{2}{137}\right)$ ، حيث $137\equiv 1 \pmod 8$

$$=\left(\frac{137}{7}\right)$$ من قانون التعاكس التربيعي وحيث $137\equiv 1 \pmod 4$

$$=\left(\frac{4}{7}\right)$$ باختزال 137 قياس 7

$$=1$$ لأن $4=2^2$ مربع كامل.

لذلك، 14 راسب تربيعي قياس 137. في الحقيقة، حلول التطابق

$$\left(\frac{55}{179}\right)=\left(\frac{5}{179}\right)\left(\frac{11}{179}\right)$$

$$=\left(\frac{179}{5}\right)\times(-1)\times\left(\frac{179}{11}\right)$$ ؛ لأن $11\equiv 179\equiv 3 \pmod 4$ و $5\equiv 1 \pmod 4$

$$=\left(\frac{4}{5}\right)\times(-1)\times\left(\frac{3}{11}\right)$$ ؛ لأن $179\equiv 3 \pmod{11}$ و $179\equiv 4 \pmod 5$

$$=1\times(-1)\times\left(\frac{3}{11}\right)$$ ؛ لأن $4=2^2$ مربع كامل

$$=1\times(-1)\times(-1)\times\left(\frac{11}{3}\right)$$ ؛لأن $3\equiv 11\equiv 3 \pmod 4$

$$=1\times(-1)\times(-1)\times\left(\frac{2}{3}\right)$$ ؛ لأن $11\equiv 2 \pmod 3$

$$=1\times(-1)\times(-1)\times(-1)$$

$$=-1$$ ؛ لأن 2 راسب غير تربيعي قياس 3.

$x^2 \equiv 14 \pmod{137}$ هي :

$$x \equiv 98 \pmod{137} \quad , \quad x \equiv 39 \pmod{137}$$

هنا مثال ثانٍ يوضح كيف أن الإشارة يمكنها أن تُغير عدة مرات.

إذاً 55 راسب غير تربيعي قياس 179.

غالباً ما يكون هناك أكثر من طريقة لاستخدام التعاكس التربيعي لحساب قيمة رمز لجندر $\left(\frac{a}{p}\right)$ ، على سبيل المثال، من خلال استخدام المساواة $\left(\frac{p}{q}\right)=\left(\frac{p-q}{q}\right)$. لذلك يمكننا حساب $\left(\frac{299}{397}\right)$ كما يلي :

$$\begin{aligned}
\left(\frac{299}{397}\right) &= \left(\frac{13}{397}\right)\left(\frac{23}{397}\right) \\
&= \left(\frac{397}{13}\right)\left(\frac{397}{23}\right) = \left(\frac{7}{13}\right)\left(\frac{6}{23}\right) \\
&= \left(\frac{13}{7}\right)\left(\frac{2}{23}\right)\left(\frac{3}{23}\right) \\
&= \left(\frac{-1}{7}\right)\times 1 \times -\left(\frac{23}{3}\right) \\
&= -1 \times -\left(\frac{2}{3}\right) \\
&= -1
\end{aligned}$$

أو يمكننا حسابها كما يلي :

$$\begin{aligned}\left(\frac{299}{397}\right)&=\left(\frac{-98}{397}\right)\\&=\left(\frac{-1}{397}\right)\left(\frac{2}{397}\right)\left(\frac{7}{397}\right)^2\\&=1\times(-1)\times(\pm1)^2\\&=-1\end{aligned}$$

طبعاً، بغض النظر عن الطريقة فالجواب النهائي نفسه.

إن قانون التعاكس التربيعي يزودنا بطريقة فعَّالة جداً لحساب رمز لجندر $\left(\frac{a}{p}\right)$، حتى للقيم الكبيرة جداً للعددين a , p .

في الحقيقة، عدد خطوات حساب $\left(\frac{a}{p}\right)$ أكثر أو أقل من أو يساوي عدد خانات p ؛ وعليه فمن الممكن حساب رموز لجندر لأعداد لها مئات الخانات.

لن نضيع الوقت بعمل مثال عدد كبير، ولكننا سنرضى بالمثال المتواضع التالي:

$$\begin{aligned}\left(\frac{37603}{48611}\right)&=\left(\frac{31}{48611}\right)\left(\frac{1213}{48611}\right)\\&=-\left(\frac{48611}{31}\right)\left(\frac{48611}{1213}\right)\\&=-\left(\frac{3}{31}\right)\left(\frac{91}{1213}\right)\\&=\left(\frac{31}{3}\right)\left(\frac{7}{1213}\right)\left(\frac{13}{1213}\right)\\&=\left(\frac{1}{3}\right)\left(\frac{1213}{7}\right)\left(\frac{1213}{13}\right)\\&=\left(\frac{2}{7}\right)\left(\frac{4}{13}\right)=1\end{aligned}$$

إذاً، 37603 راسب تربيعي قياس 48611.

إن أصعب جزء في حساب $\left(\frac{a}{p}\right)$ لا يكمن في استخدام قانون التعاكس التربيعي، ولكن في ضرورة تحليل العدد a قبل تطبيق القانون. لذلك، في مثالنا هذا، سنستهلك بعض الوقت لنعرف أن 37603 يحلل إلى $31 \cdot 1213$، وإذا كان للعدد a مئات الخانات؛ فإنه قد يكون من المستحيل تحليله. مفاجأة، من الممكن حساب قيمة $\left(\frac{a}{p}\right)$ دون مواجهة أي صعوبات في التحليل. الفكرة هي استخدام قانون التعاكس التربيعي لقلب رمز لجندر $\left(\frac{a}{p}\right)$ لأي قيمة فردية موجبة للعدد a، متجاهلين بشكل تام السؤال عن فيما إذا كان a عدداً أوليًّا أم لا. كالمعتاد، إذا كان كلا العددين a , p يطابقان 3 قياس 4، فإنك يجب أن تضع إشارة سالب.

بشكل عام، يمكننا تحديد قيمة رمز لجندر $\left(\frac{a}{b}\right)$ لأي عددين صحيحين a , b بشرط أن b عدد موجب وفردي. (هذا التعميم لرمز لجندر غالباً ما يسمى رمز جاكوبي). يمكننا حساب قيمة رمز لجندر أو جاكوبي من خلال إعادة تطبيق قانون التعاكس التربيعي العام التالي.

نظرية رقم (٢٥،٢) (قانون التعاكس التربيعي العام).

ليكن a , b عددين صحيحين فرديين موجبين

$$\left(\frac{-1}{b}\right)=\begin{cases}1, & \text{if } b\equiv 1 \pmod 4\\ -1, & \text{if } b\equiv 3 \pmod 4\end{cases}$$

$$\left(\frac{2}{b}\right)=\begin{cases}1\ , & \text{if} \quad b\equiv 1 \ or \ \ 7(\bmod 8)\\ -1\ , & \text{if} \quad b\equiv 3 \ or \ \ 5(\bmod 8)\end{cases}$$

$$\left(\frac{a}{b}\right)=\begin{cases}\left(\frac{b}{a}\right)\ , & \text{if} \quad a\equiv 1(\bmod 4)\ or\ b\equiv 1(\bmod 4)\\ -\left(\frac{b}{a}\right)\ , & \text{if} \quad a\equiv b\equiv 3(\bmod 4)\end{cases}$$

من المدهش بما فيه الكفاية، أنك إذا استخدمت هذه القوانين، وصيغة الضرب $\left(\frac{a_1a_2}{b}\right)=\left(\frac{a_1}{b}\right)\cdot\left(\frac{a_2}{b}\right)$ ، وحقيقة أن $\left(\frac{a}{b}\right)$ يعتمد فقط على قيمة a قياس b ، فإنك تنتهي بقيمة صحيحة لرمز لجندر. التحذير الوحيد، والبالغ الأهمية، هو أنه مسموح لك فقط قلب $\left(\frac{a}{b}\right)$ لقيم a الفردية الموجبة. إذا كان a زوجيًّا ، عندئذ يجب عليك أولاً تحليل قوة المقدار $\left(\frac{2}{b}\right)$ ، وإذا كانت سالبة، فيجب عليك تحليل المقدار $\left(\frac{-1}{b}\right)$.

سوف نقوم بإعطاء مثال يوضح قانون التعاكس التربيعي الجديد والمحسن من خلال إعادة حساب مثالنا السابق.

$$\begin{aligned}\left(\frac{37603}{48611}\right)&=-\left(\frac{48611}{37603}\right)\\&=-\left(\frac{11008}{37603}\right)=-\left(\frac{2^8\cdot 43}{37603}\right)\\&=-\left(\frac{43}{37603}\right)=\left(\frac{37603}{43}\right)\\&=\left(\frac{21}{43}\right)=\left(\frac{43}{21}\right)=\left(\frac{1}{21}\right)=1\end{aligned}$$

على الرغم من أن هذه الحسابات لا تبدو أقصر من سابقتها، فإنها في الحقيقة تتطلب جهداً أقل؛ لأننا لا نحتاج إلى إيجاد العوامل الأولية للعدد 37603.

لقد تحققنا من أن 37603 راسب تربيعي قياس 48611؛ لذلك فإن التطابق

$$x^2 \equiv 37603 \pmod{48611}$$

له حل (في الحقيقة، له حلان). لسوء الحظ، لم نعمل أي شيء يساعدنا على إيجاد الحلول، التي سنجد أنها $x \equiv 17173 \pmod{48611}$ و $x \equiv 31438 \pmod{48611}$. على كل حال، هناك كثير من الطرق المتقدمة التي تحل التطابق $x^2 \equiv a \pmod{p}$. ولبعض الأنواع الخاصة من الأعداد الأولية، يمكن إيجاد الحلول بشكل صريح. انظر التمرينين 25.6 و 25.7.

تمارين

(٢٥,١) استخدم قانون التعاكس التربيعي لحساب رموز لجندر التالية:

$$(a)\ \left(\frac{85}{101}\right) \qquad (b)\ \left(\frac{29}{541}\right)$$

$$(c)\ \left(\frac{101}{1987}\right) \qquad (d)\ \left(\frac{31706}{43789}\right)$$

(٢٥,٢) هل التطابق:

$$x^2-3x-1\equiv 0 \pmod{31957}$$

له أي حل؟

(مساعدة: استخدم الصيغة التربيعية لإيجاد العدد الذي تحتاجه لأخذ الجذر التربيعي بالنسبة للعدد الأولي 31957).

(٢٥,٣) بيّن أنه يوجد عدد لا نهائي من الأعداد الأولية تطابق 1 قياس 3.

(مساعدة: انظر برهان "نظرية 1 قياس 4" في الفصل 24، استخدم $A=(2p_1p_2\ldots p_r)^2+3$ ، وحاول أن تختار عدداً أوليًّا مناسباً يقسم A).

(٢٥,٤) ليكن p عدداً أوليًّا ($p\neq 2$ و $p\neq 5$)، وليكن A عدداً معطى. افرض أن p يقسم العدد A^2-5 . بيّن أن p يطابق إما 1 وإما 4 قياس 5.

(٢٥,٥) اكتب برنامجاً يستخدم التعاكس التربيعي لحساب رمز لجندر $\left(\frac{a}{p}\right)$ أو بشكل أعم، رمز جاكوبي $\left(\frac{b}{a}\right)$.

(٢٥,٦) ليكن p عدداً أوليًّا يحقق $p \equiv 3 \pmod 4$ وافرض أن a راسب تربيعي قياس p .

(a) بيّن أن $x = a^{(p+1)/4}$ حل للتطابق

$$x^2 \equiv a \pmod p$$

هذا يعطي طريقة واضحة لإيجاد جذور تربيعية قياس p لأعداد أولية تطابق 3 قياس 4.

(b) أوجد حلاً للتطابق $x^2 \equiv 7 \pmod{787}$. (يجب أن يكون جوابك واقع بين 1و 786).

(٢٥,٧) ليكن p عدداً أوليًّا يحقق $p \equiv 5 \pmod 8$ وافرض أن a راسب تربيعي قياس p .

(a) بيّن أن إحدى القيمتين :

$$x = 2a \cdot (4a)^{(p-5)/8} \qquad \text{أو} \qquad x = a^{(p+3)/8}$$

يكون حلاً للتطابق $x^2 \equiv a \pmod p$.

هذا يعطي طريقة واضحة لإيجاد جذور تربيعية قياس p لأعداد أولية تطابق 5 قياس 8.

(b) أوجد حلاً للتطابق $x^2 \equiv 5 \pmod{541}$

(أعط جواباً يقع بين 1 و 540).

(c) أوجد حلاً للتطابق $x^2 \equiv 13 \pmod{653}$

(أعط جواب يقع بين 1 و 652).

(٢٥,٨) ليكن p عدداً أوليًّا يطابق 5 قياس 8. اكتب برنامجاً لحل التطابق :

$$x^2 \equiv a \pmod p$$

استخدم الطريقة الموصوفة في التمرين السابق وطريقة التربيع المتعاقب. المخرج يجب أن يكون حلاً يحقق $0 \le x < p$. تأكد أن a راسب تربيعي ، وإذا لم يكن a راسباً تربيعيًّا فاجعل البرنامج يعطي رسالة بالخطأ . استخدم برنامجك لحل التطابقات :

$$x^2 \equiv 17 \pmod{1021},$$
$$x^2 \equiv 23 \pmod{1021},$$
$$x^2 \equiv 31 \pmod{1021}$$

(٢٥،٩) إذا كان $a^{m-1} \not\equiv 1 \pmod{m}$ ، فإن نظرية فيرما الصغرى تخبرنا أن m عدد غير أولي. من جهة أخرى ، حتى إذا كان :

$$a^{m-1} \equiv 1 \pmod{m}$$

لبعض (أو لكل) قيم a التي تحقق $\gcd(a,m)=1$ ، فإننا لا نستطيع أن نستنتج أن m عدد أولي. هذا التمرين يصف طريقة لاستخدام التعاكس التربيعي لاختبار احتمالية أن يكون العدد أوليًّا . (قارن بين هذه الطريقة واختبار رابين — ميلر Rabin-Miller المشروح في الفصل 19).

(a) يقول معيار أويلر إنه إذا كان p عدداً أوليًّا فإن :

$$a^{(p-1)/2} \equiv \left(\frac{a}{p}\right) \pmod{p}$$

استخدم التربيع المتعاقب لحساب $11^{864} \pmod{1729}$ واستخدم التعاكس التربيعي لحساب $\left(\frac{11}{1729}\right)$. هل هما متطابقان؟ ماذا يمكن أن تستنتج بشأن

احتمالية أن يكون 1729 أوليًّا؟

(b) استخدم التربيع المتعاقب لحساب المقادير

$$2^{1293336} \pmod{1293337}$$

و

$$2^{(1293337-1)/2} \pmod{1293337}$$

ماذا يمكن أن تستنتج بشأن احتمالية أن يكون 1293337 أوليًّا؟